SMĚRNICE ORGANIZAČNÍ **SMĚRNICE PRO OCHRANU OSOBNÍCH ÚDAJŮ** ČÍSLO: OS 4-2019 lipka LIPKA – ŠKOLSKÉ ZAŘÍZENÍ PRO ENVIRONMENTÁLNÍ VZDĚLÁVÁNÍ BRNO, PŘÍSPĚVKOVÁ ORGANIZACE	Nahrazuje:	OS 4 - 2018
	Zpracovala:	SSŠ Brno, Šárka Patermannová
	Schválila:	Hana Korvasová
	Směrnice je závazná pro:	všechny zaměstnance Lipky
	Platí s účinností od:	1. 9. 2019

Obecná ustanovení

Na základě ustanovení § 302 zákona č. 262/2006 Sb., zákoníku práce, nařízení EU 2016/679, obecného nařízení o ochraně osobních údajů (dále jen „GDPR“) a zákona č. 110/2019 Sb., o zpracování osobních údajů, vydávám jako statutární orgán Správce tuto směrnici.

1. Působnost směrnice

1. Tato směrnice upravuje pravidla pro ochranu osobních dat zaměstnanců a účastníků vzdělávání, Správce, jakož i dalších osob, které poskytují své osobní údaje Správci k využití (obchodní partneři, uchazeči o zaměstnání).
2. Zásady směrnice:
   - musí být vydána písemně,
   - nesmí být vydána v rozporu s právními předpisy,
   - nesmí být vydána se zpětnou účinností,
   - vzniká na dobu neurčitou,
   - je závazná pro všechny zaměstnance organizace,
   - směrnice musí být přístupná všem zaměstnancům.

2. Základní pojmy vč. klasifikačního stupně zařazení osobních údajů

1. **Osobními údaji** se v souladu s obecným nařízením o ochraně osobních údajů (dále i „Nařízení GDPR“) rozumí veškeré údaje, které umožňují přímou či nepřímou identifikaci osoby čili subjektu údajů v textové, obrazové i jiné, např. digitální podobě, a to včetně všech komunikačních údajů, kterými může být osoba identifikována v čase a místě včetně kybernetického prostoru. Zvláštní kategorie osobních údajů jsou osobní údaje, které umožňují identifikovat osoby pomocí genetických, biometrických či jiných biologických znaků osoby včetně údajů o zdravotním stavu.
2. Do zvláštní kategorie **citlivých osobních údajů** dle čl. 9 GDPR spadají údaje o:
   - národnostním, rasovém nebo etnickém původu,
   - politických postojích, členství v odborech,
   - náboženském či filozofickém přesvědčení,
   - genetické údaje, biometrické údaje,
   - zdravotním stavu,

- sexuálním životě nebo sexuální orientaci.

3. **Subjekt osobních údajů** je fyzická osoba, jejíž osobní údaje jsou předmětem zpracování.
4. **Vedením Správce** se rozumí ředitelka Lipky a její zástupci.
5. **Správcem osobních údajů** je Lipka jako právnická osoba a zároveň orgán veřejné moci v rozsahu působnosti a pravomocí školského zařízení, které zpracovává osobní údaje, případně zvláštní kategorie osobních údajů.
6. **Příjemcem osobních údajů** se rozumí fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytovány, ať už se jedná o třetí stranu, či nikoli.
7. **Zpracovatelem osobních údajů** je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který jménem Správce zpracovává osobní údaje. Pro Správce může provádět jen takové zpracovatelské operace, kterými jej Správce pověří nebo vyplývají z činnosti, pro kterou byl zpracovatel Správcem pověřen. Zpracováním osobních údajů může být pověřen i Správce, pokud takovou smlouvu uzavře.
8. **Třetí stranou** se rozumí fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který není subjektem údajů, Správcem, zpracovatelem ani osobou přímo podléhající správci nebo zpracovateli, jež je oprávněna ke zpracování osobních údajů.
9. **Pověřenec pro ochranu osobních údajů** je subjekt, který na pracovišti Správce dohlíží na dodržování opatření k ochraně osobních údajů v souladu s nařízením GDPR, poskytuje informace a poradenství zaměstnancům a zpracovatelům, kteří zpracovávají osobní údaje a spolupracuje s dozorovým úřadem v souladu s příslušnými zákonnými normami a Nařízením GDPR.
10. **Porušením zabezpečení osobních údajů** se rozumí porušení zajištění osobních údajů, které vede k náhodnému nebo úmyslnému a protiprávnímu úniku, zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů;
11. **Souhlasem se zpracováním osobních údajů** je projev vůle subjektu, kterým subjekt dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů pro daný účel.
12. **Ochranou osobních údajů** se pro účely této směrnice rozumí zajištění správy a zabezpečení osobních údajů v souladu s Nařízením GDPR a dalšími platnými právními předpisy v oblasti ochrany osobních údajů.
13. **Zpracováním osobních údajů** se pro účely této směrnice rozumí nakládání s osobními údaji, které zahrnuje shromažďování, uchovávání, používání a případné poskytování osobních údajů k různým účelům a různým stranám, jakož i veškeré úkony spojené s jejich likvidací.

3. Základní zásady zpracování a ochrany osobních údajů

1. K zajištění ochrany osobních údajů Správce musí být při jejich zpracování uplatňovány tyto zásady:

a) zajištění transparentnosti, zákonnosti a korektnosti účelu a způsobu zpracovávání osobních údajů,

b) jasné vymezení účelu, pro který jsou osobní data zpracovávána a podmínek jejich zpracování,

c) omezení rozsahu shromažďovaných osobních dat na údaje nezbytné pro naplnění účelu jejich poskytnutí subjekty údajů,

d) zajištění přesnosti a aktuálnosti zpracovávaných osobních dat tak, aby jejich obsah nevedl jejich zpracováním ke zkreslování údajů včetně z důvodu jejich zastarání,

e) omezení zpracování osobních dat pouze na dobu nezbytně nutnou pro naplnění účelu jejich uchovávání a zpracování,

f) zabezpečení osobních dat a zajištění jejich integrity, utajení a ochrany vhodnými organizačními a technickými opatřeními před ztrátou kontroly nad nimi, neoprávněným, protiprávním nebo dotčenými osobami neschváleným přístupem k nim a jejich využívání, před jejich poškozením, ztrátou či zničením, čímž vznikají rizika ztráty jejich integrity, přesnosti a bezpečnosti,

g) zamezení opakovanému požadování osobních údajů k jejich zpracování, včetně opakovaného požadování poskytování souhlasu s jejich zpracováním, leda, že by byly osobní údaje zpracovávány pro nový účel.

4. RIZIKA při zpracování OÚ

V souladu s článkem 24 a 25 nařízení jsou definovány možné oblasti nebezpečí a rizik z nich plynoucí. Tyto oblasti byly definovány zejména kontrolou dokumentace, pohovory se zaměstnanci a čerpáním z metodických materiálů[1] apod. Z těchto nebezpečí se v podmínkách Lipka můžeme potkat zejména:

- porušení vnitřních směrnic nebo pracovních postupů (porušení pracovních povinností ve smyslu ZP nebo zákona o OOÚ)
- neprovádění průběžného hodnocení systému OOÚ
- neoprávněná manipulace nebo neoprávněný přístup k OÚ
- nesprávně provedená archivace listinných dokumentů nebo nesprávně nastavená pravidla přístupů do systému informační technologie

riziko	eliminace rizika
Neznalost problematiky OOÚ	• seznámení zaměstnanců se Směrnicí • upozornění zaměstnanců na zákaz podávat jakékoli informace o účastnících vzdělávání nebo spolupracovnících cizím osobám nebo např. rodičům žáků (i soukromé telefonní číslo není možné bez souhlasu sdělit) • trvalá přístupnost této Směrnice zaměstnancům
Neaktuálnost problematiky OOÚ	• průběžná aktualizace Směrnice • průběžná informace zaměstnancům o změnách legislativy
Neoprávněná dosažitelnost zdrojů OOÚ	• neponechávat ve volně přístupných kancelářích podklady s OÚ • po pořízení dat do výpočetní techniky odhlásit program • neposkytovat výpisy z dokumentace (např. z knihy úrazů, kdy na listu je více záznamů) • osobní údaje nezveřejňovat vyvěšováním
Nesprávná archivace a ukládání	• zamezit přístupu neoprávněných osob do místnosti archivu • nezapomínat kopírované předlohy s OÚ ve stroji
Neoprávněný přístup do systému IT	• nepoužívat všeobecná hesla • vzájemné sdělování si hesla je zakázáno • neponechávat heslo tak, že je volně přístupné

[1] M. Matoušková, L. Hejlík, Osobní údaje a jejich ochrana, ASPI WK, 2. Vydání, © 2008

	• zamezit vstupu neoprávněných osob do databází (správně nastavit hierarchii přístupu)
Chybějící nebo nepřístupné archivní záznamy	• neprovádění záloh nebo kopie dat a podkladů (pravidelná záloha a její popis bude stanoven ve spolupráci s pracovníkem informační technologie), samostatná příloha Směrnice • zakládat zálohy nebo kopie na správné místo • správně označovat zálohy (datum, co, kdy, kdo) • pro zálohování dokumentů používat výhradně jednoho formátu (PDF/A) • dbát opatrnosti v případě volně přenášených CD nebo DVD a neztrácet je! • záloha na CD nebo DVD musí být opatřena heslem (pro jeho přidělení jsou stejná pravidla jako pro přístup do výpočetní techniky)

Oprávněné osoby – jedná se o zaměstnance Lipky, na které byly delegovány povinnosti při zpracování osobních údajů. Oprávněné osoby v rámci plnění svých pracovních povinností realizují opatření k ochraně osobních údajů ve smyslu této Směrnice. Za oprávněné osoby se v podmínkách Lipky se zejména považují

- ředitelka
- zástupce ředitelky
- vedoucí pracoviště
- zástupce vedoucího pracoviště
- projektový manažer
- PR manažer
- pedagogický pracovník (vedení evidence o účastnících vzdělávání apod.)
- lektor
- administrativně – organizační pracovník
- zaměstnanec, který vede personální a mzdovou agendu
- osoby pověřené vedením dokumentace o úrazech (kniha úrazů apod.)

5. Povinnosti pro naplnění ochrany OÚ

Ředitelka Lipky (správce)

- stanovuje účely zpracování osobních údajů
- stanovuje rozsah a podmínky zpracování osobních údajů přiřazením jednotlivých účelů zpracování osobních údajů k příslušným pracovním pozicím (v náplni práce)
- plní v případě potřeby oznamovací povinnost vůči Úřadu
- plní oznamovací povinnost vůči veřejnosti
- provádí 1x ročně kontrolu správnosti nakládání s osobními údaji ve spolupráci s Pověřencem pro ochranu osobních údajů
- odpovídá za řádné informování oprávněných osob o problematice OÚ nebo o změnách v legislativě
- odpovídá za zavedení změn nebo výsledků auditu do Směrnice
- provádí kontrolní činnost k dodržování zásad ochrany osobních údajů
- odpovídá za zakotvení podmínek k ochraně osobních údajů se subdodavateli

Oprávněné osoby Lipky

Oprávněné osoby jsou povinny v rámci svých pracovních povinností plnit opatření k ochraně osobních údajů, stanovená Zákonem a touto Směrnicí, dále

- zpracovávat osobní údaje za podmínek a v rozsahu stanovené Směrnicí nebo vnitřními postupy
- zachovávat mlčenlivost, a to i po skončení pracovního poměru
- vyžadovat souhlas fyzických osob, ke kterým se osobní údaje vztahují (jejich zákonných zástupců)
- informovat a poučit fyzické osoby, ke kterým se osobní údaje vztahují (jejich zákonné zástupce), o jejich právech,
- shromažďovat osobní údaje pouze v souladu se stanoveným účelem a v rozsahu nezbytném pro zpracování
- vyžadovat souhlas a prohlášení o mlčenlivosti v případě, že například kontrolní orgány chtějí nahlédnout do osobních údajů zaměstnanců, a to nad rámec jim zákonem uděleného zmocnění nebo toto odepřít;

při zpracování osobních údajů:

- zpracovávat pouze přesné osobní údaje s ohledem na účel zpracování
- v případě zjištění, že zpracovávané údaje nejsou přesné, zpracování zablokovat. O této skutečnosti informovat ředitelku Lipky
- zpracovávat osobní údaje pouze k účelům, k nimž byly shromážděny
- ukládat nosiče obsahující osobní údaje, a to v listinné i elektronické podobě, na náležitě zajištěná místa
    - uzamčená skříň
    - heslem opatřená databáze
    - cizím osobám nepřístupná spisovna nebo archiv
- neumožnit zpracování nebo nahlédnutí do osobních údajů jiné osobě
- citlivé údaje účastníků vzdělávání (nebo zaměstnanců) Lipky poskytnout pouze těm oprávněným osobám, které tyto údaje potřebují pro plnění svých pracovních povinností;

při práci s prostředky výpočetní techniky

- zajistit jedinečnost přístupových práv (nesdělovat si hesla, neponechávat napsané na papíru u PC apod.)
- řádné přihlášení a odhlášení při práci s chráněnou databází
- zálohovat databáze způsobem, který určil správce výpočetní techniky, počítačové datové sítě, a to na identifikovatelná média včetně jejich správného značení
- přístupová hesla
    - evidenci hesel vede v chráněném souboru správce počítačové datové sítě, správce informačního systému, kteří musí zpracovat postup pro jejich přidělení včetně jejich změny nebo rotace (cyklus 6 měsíců)
    - hesla přiděluje správce počítačové datové sítě a správce informačního systému nebo je využíváno automaticky generované heslo pro uživatele
- při používání přenosných prostředků informační technologie (notebooků)
    - nepředávat tento prostředek třetím osobám (ani vlastním členům rodiny)
    - neinstalovat žádné aplikace bez souhlasu správce počítačové datové sítě
    - nepoužívat přenosné prostředky bez přístupového hesla
    - učinit všechna opatření zabraňující případné ztrátě či odcizení přenosného prostředku
    - ztrátu či odcizení okamžitě nahlásit ředitelce Lipky;

Správce výpočetní techniky, správce informačního systému

Ve smyslu OOÚ je správce jednou z klíčových osob při zpracování údajů v systémech informační technologie. Správce je proto povinen:

- přidělovat zaměstnancům Lipky přístupová práva dle zadání správce OOÚ (ředitelka Lipky)

- provádět kontrolní činnost k ochraně osobních údajů zpracovávaných v rámci počítačové datové sítě, informačního systému
    - vedením evidence programového vybavení jednotlivých stanic
    - vedením evidence exspirace systémů, zejména antivirových
    - blokováním přístupu určených počítačů do veřejné sítě internet
- v případě potřebné provádění správy informační technologie nebo opravy či údržby prostředků informační technologie externím dodavatelem zajistit, aby případně instalovaná data nemohla být zneužita, není-li toto možné, zajistit problematiku OOÚ Smluvně;

6. Zákonnost zpracování osobních údajů

1. Ke zpracování osobních údajů je nutný tzv. právní důvod. Nařízení GDPR umožňuje zpracovávat osobní údaje, pokud je naplněn alespoň jeden z následujících právních důvodů:

    - subjekt údajů udělil kvalifikovaný souhlas se zpracováním osobních údajů pro jeden či více konkrétních účelů (čl. 6 odst. 1 písm. a) Nařízení GDPR),

    - zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů (čl. 6 odst. 1 písm. b) Nařízení GDPR),

    - zpracování je nezbytné pro splnění právní povinnosti, která se na Správce vztahuje (čl. 6 odst. 1 písm. c) Nařízení GDPR),

    - zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby (čl. 6 odst. 1 písm. d) Nařízení GDPR),

    - zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je Správce pověřen (čl. 6 odst. 1 písm. e) Nařízení GDPR),

    - zpracování je nezbytné pro účely oprávněných zájmů Správce či třetí strany s výjimkou případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů (čl. 6 odst. 1 písm. f) Nařízení GDPR).

2. Pokud zpracování pro jiný účel, než pro který byly osobní údaje původně shromážděny, není založeno na souhlasu subjektu údajů nebo na jiných právních důvodech, je v zájmu zjištění toho, zda je zpracování pro jiný účel slučitelné s účely, pro něž byly osobní údaje původně shromážděny, nutné zohlednit mimo jiné:

    - jakoukoli vazbu mezi účely, kvůli nimž byly osobní údaje shromážděny a účely zamýšleného dalšího zpracování,

    - okolnosti, za nichž byly osobní údaje shromážděny, zejména pokud jde o vztah mezi subjekty údajů a Správcem,

    - povahu osobních údajů, zejména zda jsou zpracovávány zvláštní kategorie osobních údajů podle čl. 9 Nařízení GDPR nebo osobní údaje týkající se rozsudků v trestních věcech a trestných činů podle čl. 10 Nařízení GDPR,

    - možné důsledky zamýšleného dalšího zpracování pro subjekty údajů,

    - existenci vhodných záruk, mezi něž může patřit šifrování nebo pseudonymizace.

7. Zpracování zvláštních kategorií osobních údajů

1. Zakazuje se zpracování osobních údajů, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.

2. Výjimky z tohoto ustanovení jsou uvedeny v čl. 9 Nařízení GDPR, a to zejména z následujících důvodů:

   - subjekt údajů udělil výslovný souhlas se zpracováním těchto osobních údajů pro jeden nebo více stanovených účelů, s výjimkou případů, kdy právo Unie nebo členského státu stanoví, že zákaz uvedený v odstavci 1 nemůže být subjektem údajů zrušen,

   - zpracování je nezbytné pro účely plnění povinností a výkon zvláštních práv Správce nebo subjektu údajů v oblasti pracovního práva a práva v oblasti sociálního zabezpečení a sociální ochrany, pokud je povoleno právem Unie nebo členského státu nebo kolektivní dohodou podle práva členského státu, v němž se stanoví vhodné záruky týkající se základních práv a zájmů subjektu údajů,

   - zpracování se týká osobních údajů zjevně zveřejněných subjektem údajů,

   - zpracování je nezbytné pro určení, výkon nebo obhajobu právních nároků,

   - zpracování je nezbytné z důvodu významného veřejného zájmu na základě práva Unie nebo členského státu, které je přiměřené sledovanému cíli, dodržuje podstatu práva na ochranu údajů a poskytuje vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů,

   - zpracování je nezbytné pro účely preventivního nebo pracovního lékařství, pro posouzení pracovní schopnosti zaměstnance,

   - zpracování je nezbytné pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely v souladu s čl. 89 odst. 1 Nařízení GDPR na základě práva Unie nebo členského státu, které je přiměřené sledovanému cíli, dodržuje podstatu práva na ochranu údajů a poskytuje vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů.

8. Zpracování osobních údajů Správce prostřednictvím zpracovatele

1. Správce osobních údajů může pověřit zpracováním osobních údajů zpracovatele. Zpracovatel může pro Správce zpracovávat osobní údaje pouze na základě zpracovatelské smlouvy, která musí být písemná. V této smlouvě musí být vždy jednoznačně stanoven předmět a doba trvání zpracování osobních údajů, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů a veškeré povinnosti a práva Správce a zpracovatele.

2. Ve smlouvě musí být dle čl. 28 Nařízení GDPR stanoveny zejména následující povinnosti zpracovatele:

   - že zpracovatel přijme všechna bezpečnostní, technická, organizační a jiná opatření požadovaná v čl. 32 Nařízení GDPR, přitom přihlédne ke stavu techniky, nákladům na provedení, povaze zpracování, rozsahu zpracování, kontextu zpracování a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob,

   - že zpracovatel nezapojí do zpracování žádné další osoby bez předchozího písemného souhlasu Správce,

   - že zpracovatel zpracovává osobní údaje pouze na základě doložených pokynů Správce (vč. předání údajů do třetích zemí a mezinárodním organizacím) a že výjimkou jsou pouze případy, kdy jsou určité povinnosti zpracovateli uloženy přímo právním předpisem,

   - že zpracovatel zajistí, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti,

   - že zpracovatel bude Správci bez zbytečného odkladu nápomocen při plnění povinností Správce, zejména povinnosti reagovat na žádosti o výkon práv subjektů údajů, povinnosti ohlašovat případy porušení zabezpečení osobních údajů dozorovému úřadu dle čl. 33 Nařízení GDPR, povinnosti oznamovat případy porušení zabezpečení osobních údajů subjektu údajů dle čl. 34 Nařízení GDPR, povinnosti posoudit vliv na ochranu osobních údajů dle čl. 35 nařízení a povinnosti provádět předchozí konzultace dle čl. 36 nařízení, a že za tímto účelem zpracovatel zajistí nebo přijme vhodná technická a organizační opatření, o kterých ihned informuje Správce,

   - že zpracovatel po ukončení poskytování služeb spojených se zpracováním řádně naloží se zpracovávanými osobními údaji, např. že všechny osobní údaje vymaže, nebo je vrátí Správci a vymaže existující kopie apod.,

   - že zpracovatel poskytne Správci veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené Správci právními předpisy,

   - že zpracovatel umožní kontroly, audity či inspekce prováděné Správcem nebo jiným příslušným orgánem dle právních předpisů,

   - že zpracovatel poskytne bez zbytečného odkladu nebo ve lhůtě, kterou stanoví Správce, součinnost potřebnou pro plnění zákonných povinností Správce spojených s ochranou osobních údajů, jejich zpracováním a s plněním smlouvy o zpracování osobních údajů.

3. Zpracovatelská smlouva musí obsahovat vhodné záruky splnění povinností zpracovatele; jedná se zejména finanční záruky nebo využití zástavního práva, a to nejen za porušení jednotlivých povinností zpracovatele uvedených ve smlouvě, ale především pro případy, kdy byla v důsledku jednání zpracovatele správci uložena pokuta. Pro případ závažného porušení povinností zpracovatele (např. předání zpracovávaných údajů třetí osobě) by mělo být ve smlouvě upraveno právo Správce odstoupit od smlouvy. Dále by mělo být ve všech smlouvách vždy zakotveno právo Správce smlouvu vypovědět včetně stanovení přiměřené výpovědní lhůtu.

9. Shromažďování údajů

1. Správce shromažďuje a zpracovává pouze údaje, které:
    - jsou nezbytné pro vedení personální a mzdové agendy Správce, souvisejí s pracovním a mzdovým zařazením zaměstnanců, sociálním, sociálním a zdravotním pojištění (např. dosažené vzdělání, délka praxe, funkční zařazení apod.),
    - jsou nezbytné pro identifikaci účastníka vzdělávání ze zákona, ochrany oprávněných zájmů, plnění smluvních povinností a na základě souhlasu se zpracováním osobních údajů (jméno, příjmení, datum narození, místo narození, rodné číslo, státní příslušnost, bydliště, údaj o zákonném zástupci, údaje o zdravotním stavu, zdravotní pojišťovnu apod.),
    - jsou nezbytné pro jednoznačnou identifikaci zákonných zástupců účastníků vzdělávání v souladu se zákonem, plněním smluvních povinností a na základě souhlasu se zpracováním osobních údajů (jméno, příjmení, datum narození, bydliště, telefonní kontakt, email, číslo bankovního účtu pro potřeby plateb poplatků Správci, další údaje nezbytné pro vydání správního rozhodnutí apod.),
    - jsou nezbytné pro plnění smluvních povinností Správce ve vztahu ke svým obchodním partnerům a povinností Správce vyplývajících ze zvláštních právních předpisů (vedení účetnictví, daňového účetnictví apod.),
    - jsou nezbytné pro identifikaci klientů e-shopu, plnění smluvních povinností a vedení uživatelského účtu na e-shopu (jméno, příjmení, název, datum narození, bydliště, sídlo, IČO, telefon, email apod.),
    - jsou nezbytné pro identifikaci osob oprávněných vyzvedávat nezletilé děti a účastníky z akcí Správce (jméno, příjmení a vztah k dítěti, účastníkovi akce),
2. Přesná specifikace rozsahu zpracovávaných osobních údajů včetně důvodů zpracování je uvedena v záznamech o činnostech zpracování, které tvoří přílohu této směrnice.
3. Osobní údaje Správce uchovává v listinné i v elektronické podobě.
4. V **listinné** podobě Správce eviduje a uchovává osobní údaje

    <u>zaměstnanců Správce</u>
    - v jeho osobním spise umístěném v uzamykatelné kanceláři mzdové účetní, do které má přístup pouze vedení Správce (ředitel, zástupce ředitele) a mzdová účetní,
    - v knize úrazů zaměstnanců uložené v uzamykatelné skříni na pracovišti s povoleným přístupem pouze vedoucího pracoviště nebo jeho zástupce, kteří do knihy provádí zápis,
    - a dále v krátkodobé dokumentaci uložené v kanceláři příslušného zaměstnance, který danou dokumentaci potřebuje pro řádný výkon svých pracovních povinností, v uzamykatelné skříni, do které má přístup pouze vedení Správce (ředitel, zástupce ředitele) a příslušný zaměstnanec,

    <u>zákonných zástupců účastníků</u>
    - ve spisu založeném v rámci přijímání zájemce o vzdělávání umístěné v uzamykatelné kanceláři vedoucího příslušného pracoviště, v uzamykatelné skříni s povoleným přístupem pouze vedení Správce,

    <u>účastníků vzdělávání</u>
    - v matrice školského zařízení a dokumentech vedených v souladu s ustanovením školského zákona, nebo v materiálu, který plní obdobnou funkci, umístěných v uzamykatelné kanceláři vedoucího příslušného pracoviště, v uzamykatelné skříni s povoleným přístupem pouze vedení Správce,

- v knize úrazů zaměstnanců uložené v uzamykatelné skříni na pracovišti s povoleným přístupem pouze vedoucího pracoviště a jeho zástupce, kteří do knihy provádí zápis,
- a dále v krátkodobé dokumentaci uložené v kanceláři příslušného zaměstnance, který danou dokumentaci potřebuje pro řádný výkon svých pracovních povinností, v uzamykatelné skříni, do které má přístup pouze vedení Správce (ředitel, zástupce ředitele) a příslušný zaměstnanec,

obchodních partnerů

- v dokumentaci uložené v kanceláři hlavní ekonomky Správce v uzamykatelné skříni, do které má přístup pouze vedení Správce a zaměstnanci ekonomického oddělení

osob oprávněných vyzvedávat nezletilé děti a účastníky z akcí Správce

- v dokumentaci umístěné v uzamykatelné kanceláři vedoucího příslušného pracoviště, v uzamykatelné skříni s povoleným přístupem pouze vedení Správce,
- v krátkodobé dokumentaci uložené v kanceláři příslušného zaměstnance, který danou dokumentaci potřebuje pro řádný výkon svých pracovních povinností, v uzamykatelné skříni, do které má přístup pouze vedení Správce (ředitel, zástupce ředitele) a příslušný zaměstnanec.

5. V **elektronické** podobě jsou uloženy osobní údaje
   - zaměstnanců, a to informace nezbytné pro vedení personální a mzdové agendy Správce, na místní síti správce v části, do které má přístup jen mzdová účetní a vedení Správce po zadání *přihlašovacího jména a hesla*. Pro správu osobních údajů Správce používá speciální mzdový systém,
   - účastníků vzdělávání, jejich zákonných zástupců a osob oprávněných vyzvedávat děti z akcí Správce, na místní síti správce v části, do které má přístup jen vedení Správce a příslušný pedagog po zadání *přihlašovacího jména a hesla,*
   - obchodních partnerů, a to na místní síti správce v části, do které má přístup jen ekonomka a vedení Správce po zadání *přihlašovacího jména a hesla*. Pro správu osobních údajů Správce používá speciální účetní systém,
   - klientů e-shopu a uživatelů e-shopu, a to v databázi uživatelů a objednávek e-shopu a dále na sdíleném datovém úložišti Správce, do kterého má přístup pouze vedení Správce a pověření zaměstnanci po zadání *přihlašovacího jména a hesla.*

6. Osobní údaje se uchovávají pouze po dobu, která je nezbytná k účelu jejich zpracování a po dobu nezbytné archivace. Lhůty pro ukládání osobních údajů jsou specifikovány v záznamech o činnostech zpracování.
7. Správce shromažďuje a zpracovává jen ty osobní údaje, které odpovídají stanovenému účelu a rozsahu zpracování. Zpracovávají se pouze pravdivé a přesné osobní údaje. Pro statistické účely je nutné osobní údaje anonymizovat. Je třeba zamezit neoprávněnému přístupu ke shromážděným údajům.

9. Přístup k osobním údajům

1. K osobním údajům mají přístup pouze zaměstnanci, kteří jej potřebují pro řádný výkon svých pracovních povinností.
2. K osobním údajům zaměstnanců má přístup výhradně vedení Správce (ředitel, zástupce ředitele) a mzdová účetní. Právo nahlížet do osobního spisu zaměstnance má výhradně příslušný zaměstnanec, činit si z něho výpisky a pořizovat si stejnopisy dokladů v něm obsažených, a to

na náklady zaměstnavatele (§ 312 zákoníku práce), případně osoby, o kterých tak výslovně stanoví zvláštní právní předpis. Osobní údaje se předávají orgánům veřejné správy, zdravotní pojišťovně a případně zpracovatelům osobních údajů, a to vždy pouze pro naplnění účelu zpracování, tedy pokud takovou povinnost ukládá Správci zákon nebo pokud je předání nezbytné pro plnění povinností Správce jakožto zaměstnavatele.

3. K osobním údajům účastníků vzdělávání a jejich zákonných zástupců
   - ve školní matrice – mají přístup pedagogičtí pracovníci školy a vedení Správce,
   - do údajů o zdravotním stavu účastníků vzdělávání, zpráv o vyšetření ve školním poradenském zařízení, lékařských zpráv – mají přístup pedagogičtí pracovníci školské zařízení, kteří dítě/účastníka vzdělávání přímo vzdělávají, ředitel a zástupce ředitele Správce.
   - do spisu vedeném ve správním řízení – mají přístup účastníci správního řízení, vedení Správce a osoba, která je zmocněna s úředním spisem pracovat po dobu řízení.

   Právo nahlížet do osobního spisu či si pořizovat výpisy a opisy má výhradně účastník nebo jeho zákonný zástupce. Osobní údaje účastníků vzdělávání jsou předávány zpracovatelům osobních údajů výhradně, pokud je toto předání v souladu s účelem zpracování, především poskytovateli IT služeb či poskytovateli zdravotních služeb.
4. K osobním údajům obchodních partnerů má přístup pouze vedení Správce (ředitel, zástupce ředitele) a účetní. Osobní údaje smluvních partnerů jsou předávány zpracovatelům osobních údajů výhradně, pokud je toto předání v souladu s účelem zpracování, především poskytovateli IT služeb.
5. K osobním údajům klientů e-shopu a uživatelů e-shopu má přístup jen vedení Správce a zaměstnanci pověřený správou e-shopu a vyřizováním objednávek z e-shopu.
6. Osobní údaje mohou být dále předány orgánům státní správy, jestliže o jejich zpřístupnění požádají v souladu se zvláštními právními předpisy, za podmínek stanovených zákonem a při výkonu své činnosti.
7. Zaměstnanec, který není oprávněn nakládat s osobními údaji některé kategorie osobních údajů je povinen zdržet se jakéhokoliv jednání, které by mu přístup k daným osobním údajům umožnilo. Jestliže se Zaměstnanec dostane do kontaktu s osobními údaji, které není oprávněn zpracovávat, nebo s osobními údaji, které nejsou uloženy a zabezpečeny v souladu s touto směrnicí či GDPR, případně bude informován o jiném porušení zabezpečení osobních údajů, je o tomto povinen bezodkladně a informovat vedení Správce.

10. Souhlas k zpracováním osobních údajů

1. Ke zpracování osobních údajů a citlivých osobních údajů nad rozsah daný právními předpisy je nezbytný souhlas osoby, jejíž osobní údaje jsou zpracovávány. Správce před zahájením zpracování osobních dat prokazatelně zajistí plnou informovanost těchto subjektů v rozsahu daném GDPR a poučení o jejich právech.

11. Organizační opatření k ochraně osobních údajů v organizaci a koncepce s jejich nakládáním vč. procesu zvládání incidentů

1. Všichni zaměstnanci, na něž se vztahuje tato směrnice, jsou povinni dodržovat při shromažďování, evidenci a zpracování osobních údajů ustanovení GDPR, který mimo jiné stanoví, co se těmito údaji a manipulací s nimi rozumí.

2. Veškeré listinné dokumenty obsahující osobní údaje musí být uloženy na místě k tomuto určeném tak, jak je popsáno ve čl. 7. této směrnice s výjimkou doby, po kterou s těmito osobními údaji pracuje pověřená osoba.
3. Pověřená osoba je povinna přijmout veškerá opatření nezbytná pro ochranu a zabezpečení osobních údajů, se kterými pracuje, tak aby nemohlo dojít k jejich ztrátě, zničení, zcizení či zneužití. Pověřená osoba je především povinna mít osobní údaje uloženy na pracovním místě a pod svým dohledem. Při opuštění pracovního místa se musí Pověřená osoba ujistit, že jsou osobní údaje zabezpečeny před neoprávněným přístupem, a to uložením osobních údajů do uzamykatelného kontejneru nebo uzamčením místnosti, ve které se osobní údaje nachází.
4. Pověřená osoba je oprávněna předat osobní údaje pouze subjektu osobních údajů nebo osobě, která je k tomuto výslovně oprávněna zákonem nebo prokazatelným pověřením subjektu osobních údajů. V případě pochybností je pověřená osoba povinna obrátit se na vedení Správce. O předání či zpřístupnění osobních údajů jakékoliv osobě bude proveden písemný záznam podepsaný zaměstnancem, který přístup k osobním údajům umožnil, a osobou, které byl přístup k osobním údajům umožněn.
5. Každá pověřená osoba je povinna zachovávat mlčenlivost o osobních údajích, které zpracovává v rámci plnění svých pracovních povinností a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů. Povinnost mlčenlivosti trvá i po ukončení pracovněprávního vztahu.
6. Přístup k osobním údajům v elektronické podobě je zajištěn individuálními přihlašovacími jmény a hesly, které pověřeným osobám vydává vedení Správce.
7. Pověřená osoba je povinna zachovávat přihlašovací údaje v tajnosti a přijmout taková opatření, aby nemohlo dojít k jejich zcizení či zneužití. Zakázáno je především předávání přihlašovacích údajů jinému zaměstnanci, třetí osobě, zapisování přihlašovacích údajů na veřejně dostupná místa či povolení automatického ukládání hesel v ICT zařízení.
8. V případě ztráty přihlašovacích údajů, nebo byť jen podezření z jejich zneužití je pověřená osoba povinna toto bezodkladně ohlásit vedení Správce/správci ICT sítě/, který zajistí bezodkladnou deaktivaci přihlašovacích údajů a vydání přihlašovacích údajů nových.
9. Pověřená osoba je povinna odhlásit se ze systému při ukončení práce s elektronickou databází osobních údajů, nebo při jejím přerušení a opuštění pracoviště.
10. Písemnosti a mobilní/externí/přenosné technické nosiče informací, jimiž disponují pověřené osoby a které obsahují osobní údaje chráněné podle této směrnice, musí být uchovávány pouze v uzamykatelných skříních či zásuvkách na pracovištích Správce, případně na jiných bezpečných místech nebo musí být zabezpečeny systémem přístupových hesel. Pokud uvedené řešení není možné, musí být přijata taková organizační a bezpečnostní opatření, která osobní údaje řádně zabezpečí.
11. Počítače a další technické prostředky, na nichž jsou uložena data obsahující osobní údaje chráněné podle této směrnice, musí být povinně zabezpečeny před volným přístupem neoprávněných osob přístupovými hesly, šifrováním či uzamčením.
12. Kopie osobních údajů chráněných podle této směrnice musí být pořizovány na technické nosiče informací podle provozních pravidel stanovených pro jednotlivá zpracování údajů a uchovávány v uzamykatelných skříních na pracovištích Správce, případně na jiných bezpečných místech.
13. V případě, kdy zaměstnanec Správce zjistí nebo nabude podezření, že by mohlo dojít nebo že došlo k porušení zabezpečení osobních údajů, je povinen to neprodleně oznámit vedení Správce a pověřenci. Vedení Správce bez odkladu přijme nezbytná opatření, aby nedošlo k poškození, ztrátě, zcizení či jinému zneužití osobních údajů.
14. Ohlašování případů porušení zabezpečení osobních údajů dozorovému orgánu dle čl. 33 Nařízení GDPR a oznamování případů porušení ochrany osobních údajů subjektu údajů dle čl. 34 Nařízení GDPR provádí pověřenec.

11. Závěrečná ustanovení

1. Porušení povinností dle této směrnice se považuje za podstatné porušení pracovních povinností.
2. Kontrolou provádění ustanovení této směrnice je pověřen statutární orgán Správce.
3. Směrnice nabývá účinnosti dne 1. září 2019